

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平5-94458

(43)公開日 平成5年(1993)4月16日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/21	3 4 0 A	7218-5L		
G 0 6 K 17/00		L 8623-5L		
G 0 7 D 9/00	4 3 6 Z	8513-3E		
		7130-3E	G 0 7 F 7/ 08	B
		7117-5K	H 0 4 L 9/ 02	A

審査請求 未請求 請求項の数 4(全 22 頁) 最終頁に続く

(21)出願番号 特願平3-278831

(22)出願日 平成3年(1991)9月30日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72)発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72)発明者 長谷部 高行

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(74)代理人 弁理士 真田 有

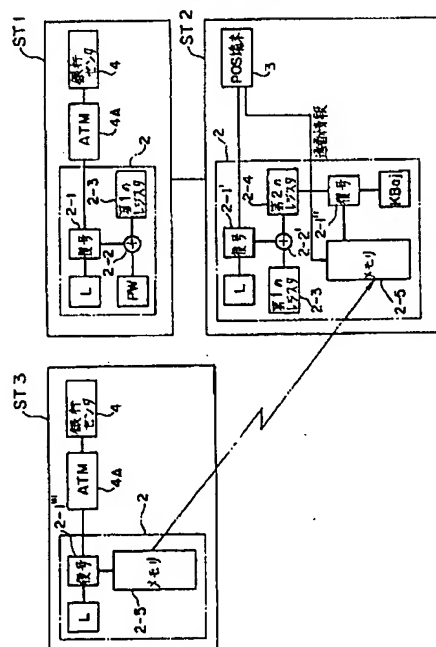
(54)【発明の名称】 電子財布システムの鍵管理方式

(57)【要約】

【目的】 本発明は、銀行センタ、現金自動支払い装置、ICカード及び店舗取引端末で構成される電子財布システムを正しく運用するための認証手段に必要な鍵管理方式に関し、銀行鍵を個人毎にユニークにし、更にこれを時間可変な鍵とすることによって、高い安全性を確保できるようにすることを目的とする。

【構成】 電子財布システムの鍵管理方式において、ICカード2内のメモリ2-5に、暗号化セッション鍵を複数種類記憶しておき、ICカード2が店舗取引端末3側から第2の暗号化パラメータを受け取る際に、メモリ2-5のアドレス情報を有する通番情報を受け取り、この通番情報に対応するメモリ2-5のアドレスをアクセスして、対応するアドレスに記憶された暗号化セッション鍵を出力して、第2レジスタ2-4の値でこの出力を復号し、目的の認証用の鍵を得るように構成する。

本発明の原理説明図



【特許請求の範囲】

【請求項1】 銀行センタ（4）、現金自動支払い装置（4A）、ICカード（2）及び店舗取引端末（3）から構成され、

該銀行センタ（4）で、マスタ鍵を用いて該銀行センタ（4）が生成する第1のパラメータを暗号化し、該銀行センタ（4）より現金自動支払い装置（4A）を経由してユーザの該ICカード（2）へ配送すると、

ユーザは該現金自動支払い装置（4A）より配送された暗号化パラメータを該ICカード（2）に取り込み、該ICカード（2）内のマスタ鍵で復号し、銀行発行の第1のパラメータを得、更にこのパラメータとユーザが管理するパスワードとを、該ICカード（2）内で加算し、この結果を第1のレジスタ（2-3）に書き込んで、

その後、ユーザが商店で買物を行ない、該店舗取引端末（3）で買物金額を支払う際に、該ICカード（2）を該店舗取引端末（3）のカードリーダーへ挿入すると、該店舗取引端末（3）側で予め銀行センタマスタ鍵で暗号化した第2のパラメータを該ICカード（2）に対して送り、

該ICカード（2）において受信した第2の暗号化パラメータを内蔵のマスタ鍵で復号し、得られた該第2のパラメータを該第1のレジスタ（2-3）の値に対して加算し、その結果を該第2のレジスタ（2-4）に格納して、

該ICカード（2）内のメモリ（2-5）に記憶された暗号化セッション鍵を用いて、該第2レジスタ（2-4）の値で復号し、目的の認証用の鍵を得るようにした電子財布システムの鍵管理方式において、

該ICカード（2）内の該メモリ（2-5）に、該暗号化セッション鍵を複数種類記憶しておき、

該ICカード（2）が該店舗取引端末（3）側から該第2の暗号化パラメータを受け取る際に、該メモリ（2-5）のアドレス情報を有する通番情報を受け取り、この通番情報に対応する該メモリ（2-5）のアドレスをアクセスして、対応するアドレスに記憶された該暗号化セッション鍵を出力して、該第2レジスタ（2-4）の値でこの出力を復号し、目的の認証用の鍵を得ることを特徴とする、電子財布システムの鍵管理方式。

【請求項2】 該ICカード（2）の該メモリ（2-5）へ一連の暗号化セッション鍵を書き込む場合、該銀行センタ（4）よりマスタ鍵で該暗号化セッション鍵を暗号化し、このデータを該現金自動支払い装置（4A）を通じて、該ICカード（2）に与え、

該ICカード（2）は受信したデータをマスタ鍵で復号し、得られた一連の暗号化セッション鍵データを順次該メモリ（2）に格納することを特徴とする、請求項1記載の電子財布システムの鍵管理方式。

【請求項3】 該銀行センタ（4）が暗号化セッション

鍵を発行する場合、一定の時間単位に対応する複数個の暗号化セッション鍵を該現金自動支払い装置（4A）経由で該ICカード（2）に配送することを特徴とする、請求項1記載の電子財布システムの鍵管理方式。

【請求項4】 該銀行センタ（2）が該店舗取引端末（3）に対して第2の暗号化パラメータを送る場合、該銀行センタ（2）よりマスタ鍵で暗号化した第2のパラメータを一定の時間単位に対応させて複数個のデータを該店舗取引端末（3）へ送ることを特徴とする、請求項1記載の電子財布システムの鍵管理方式。

【発明の詳細な説明】

【0001】（目次）

産業上の利用分野

従来の技術（図7、図8）

発明が解決しようとする課題（図9～図14）

課題を解決するための手段（図1）

作用（図1）

実施例（図2～図6）

発明の効果

【0002】

【産業上の利用分野】本発明は、銀行センタ、銀行ATM（現金自動支払い装置）、ICカード及び商店POS端末（店舗取引端末）の要素から構成される電子財布システムにおいて、これらの構成要素を正しく運用するための認証手段に必要な鍵管理方式に関する。

【0003】近年、テレホンカードに代表されるように、現金を直接支払わず、予め現金を各種のプリペイドカードに替えて、電話の通話料金を支払ったり、電車の切符を購入したり、食券を購入したりするプリペイドカードシステムが普及しつつある。しかし、このような現状のカードシステムでは、特定のサービスや品物のみに利用可能であるため、一般の商品購入には不向きである。

【0004】そこで、万能プリペイドカードとして期待されるのが、電子財布システムである。これは銀行、各種金融機関が顧客に予めICカードを発行しておき、顧客が買物をする際、ATM（現金自動支払機）より、現金の代わりに金額データをICカードに書き込み、顧客は店で買物した金額をこのICカードにより支払うシステムである。

【0005】かかる電子財布システムは顧客が現金を所有する必要がない点、及び店から銀行に売上げ金を運搬する現金輸送車が不要である点等から安全性が高く、効率的である。しかし、これはあくまでもATM、ICカード及び店のPOS（Point of Sale）システムが全て安全であることが前提である。

【0006】

【従来の技術】図7はICカードを用いたプリペイドカード・システムの従来方式のシステム構成図である。このシステムは、ICカード81、ICカード81を持つ

3

ているユーザが買物をする店舗に置く店舗取引端末（POS端末）82、銀行センタ83からなる。

【0007】銀行センタ83には、ICカード81を保有するユーザの個人口座84、カード・ユーザが自身のカードに入金した金額データを格納しておく個人カード残高ログファイル85、複数のカードにユーザが入金した金額の合計額を格納しておく未決済資金ファイル86、各店舗の一定期間のカード売上合計額を未決済資金ファイルから資金移動する店舗口座87がある。未決済資金ファイル86は銀行センタ83で一つまたは複数存在する。また、個人口座84および個人カード残高ファイル85はICカード81を保有する各個人に対応して存在し、また、店舗口座87は各店舗に対応して存在する。

【0008】ICカード81には、残高格納レジスタ88があり、該ICカード81で使用可能な金額が格納されている。また、店舗取引端末（POS端末）82には、該端末での売上を格納する売上データ89が存在する。

【0009】カード・ユーザは、自身のICカード81を使用するにあたって、まず、ICカード81に入金する。入金の際には、カードのキーパッドから暗証番号を入力し、該ICカード81を活性化させたうえ、ATM90を介して銀行センタ83にアクセスする。カードに入金したい金額が個人口座84の残高以内ならば、この金額をカード残高と加算して加算結果をICカード81の残高格納レジスタ88にATM90を介して書き込む（カードへの入金金額91）。これと同時に、カード残高を銀行センタ83の個人カード残高ログファイル85に書き込む。

【0010】この個人カード残高ログファイル85はICカード81への不正行為防止に使用できる。すなわち、カード・ユーザが次に入金にきたときにはICカード81の残高は該個人カード残高ログファイル85に書き込まれている金額と同じかあるいは少ないはずなので、もしICカード81の残高格納レジスタ88の金額の方が個人カード残高ログファイル85よりも多いならばICカード81を不正改ざんしたとみなすことができる。また、個人カード残高ログファイル85に格納されている金額は、カードを破損した場合などにガード・ユーザに対して保証する保証金額となる。

【0011】ICカード81で買物をする場合には、店舗取引端末82に買物金額を入力し、さらにICカード81を店舗取引端末82に挿入し、ICカード81のキーパッドから暗証番号を入力することによりICカード81を活性化（買物のための活性化92）。これによって、店舗取引端末82がICカード81の残高格納レジスタ88の残高から買物金額を差し引いて残高額を更新する（残高減算93）とともに、売上データ89に買物金額を加算する。すなわち、ICカード81のカー

4

ド・ユーザがA銀行に口座を有している場合には、売上データ89のうちA銀行について、金額aに買物金額を加算して更新する。

【0012】店舗取引端末82では、以上の方法によって売上げ金額を売上データ89に加算していき、一定期間ごとに売上データ89の金額を暗号化して銀行センタ83に送る。すなわち、一定期間が経った時点で、銀行ごとの売上金額（例えばA銀行ならば金額a）を暗号化し、売上（請求）データ94として該銀行センタ（例えばA銀行の銀行センタ）に送る。銀行センタ83は送られてきた売上（請求）データ94を復号し、その金額を未決済資金ファイル86から店舗口座87に移す。

【0013】図8は店舗取引端末における従来の売上合算データの更新とICカード残高の更新の説明図である。買物を行なう場合には、店舗取引端末82にICカード81を挿入し、暗証番号によりICカード81を活性化し、買物金額95を店舗取引端末82から入力する。この買物金額95は、店舗取引端末82の加算器96およびICカード81の減算器97の入力となるとともに、ICカード81の金額表示ディスプレイ98に出力される。これによって、ICカード81のユーザは買物金額95の入力に誤りがないかを判断することができる。店舗取引端末82の加算器96のもう一つの入力には売上合算データ99である。買物金額95が入力されると、加算器96によってそれまでの売上合算データ99に該買物金額95を加算し、売上合算データ99を更新する。一方、ICカード81の減算器97のもう一つの入力は残高格納レジスタ88の値である。買物金額95が入力されると、減算器97によって残高格納レジスタ88の値から買物金額95を減算し、再び残高格納レジスタ88に格納し、残高を更新する。

【0014】以上のように、従来のプリペイドカード・システムでは、ICカードの暗証番号入力により本人以外の使用を不可能にするためのアクセス制御と、店舗—銀行センタ間の回線における盗聴を防止するための暗号化が安全対策として行なわれている。

【0015】

【発明が解決しようとする課題】しかしながら、上記の従来の方式では、店舗端末での不正に対する防御はなされておらず、プリペイドカード・システム全体としての安全性に問題がある。そこで、次のようなシステムが考えられる。

【0016】図9はそのシステム構成図である。ICカード2および店舗取引端末3についての構成を説明する。ICカード2は、残高格納レジスタ8および減算器20、金額表示部21からなる。また、店舗取引端末3は、売上データ22、加算器23、暗号化部24、暗号化部25、比較器26、銀行鍵27からなる。そして、売上データ22は、売上合算データ28および認証子29で構成する。

5

【0017】カード・ユーザが買物を行ないICカードで支払いをする際に、店舗取引端末3の売上データ22の更新およびICカード2の残高格納レジスタ8の更新を行ない、これに加えて不正防止処理を行なう。

【0018】まず、ICカード2による支払いに先立ち、店舗取引端末3は暗号化部24によって、売上データ22のなかの売上合算データ28を銀行鍵27で暗号化し、その結果を比較器26に出力する。銀行鍵27は、該店舗がICカードによる販売で提携している複数の銀行について銀行ごとに用意してある暗号化用の鍵である。比較器26では、この暗号化済みのデータと認証子29を比較し、認証子29作成時の売上合算データ28が改ざんされているか否かを判定する。すなわち、比較器26で暗号化済みデータと認証子29が一致していればデータの改ざんはなされていないと判断し、ICカード2による支払い処理を実行する。一方、一致していない場合にデータを改ざんしたものと判断し、ICカード2による支払い処理は行なわずに、不正行為あるいはエラーが生じたとしてオペレータに通知する。

【0019】改ざんされていないと判定された場合には、次の処理を実行する。まず、店舗取引端末3のキーボード等から買物金額9を入力する。そして、この買物金額9と売上データ22中の売上合算データ28とを加算し、加算結果を売上合算データ28に格納して、これまでの売上合算データを更新する。また、加算結果は、暗号化部25へも入力される。暗号化部25で、この新売上合算データを銀行鍵27で暗号化し、その結果を認証子29に格納して、認証子29の更新を行なう。

【0020】認証子29を作成するための暗号化処理（認証子生成）は一般の暗号化と同様の処理（例えばF E A Lアルゴリズムなど）で実行する。被暗号文のうちの何ビットかを暗号化し認証文とする。例えば、128ビットの被暗号文のうちの64ビットを暗号化し認証文とする。このため、認証文から被暗号文を逆生成することはできない。

【0021】一方、ICカード2にも買物金額9が入力される。買物金額9は、金額表示部21に表示されたうえ、減算器20の入力となる。減算器20のもう一つの入力は残高格納レジスタ8の残高データである。減算器20は、該残高データから今回の買物金額9を減算し、その結果を残高格納レジスタ8に格納して、残高データを更新する。

【0022】以上に説明した第1の例では、店舗取引端末3において売上合算を求めるときに売上合算データの暗号化を行ない、売上合算データとともに認証子として格納したうえ、次回、売上合算を行なう際に前回計算し格納した売上合算データを再び暗号化し、前回格納した認証子と比較することにより、店舗取引端末3において売上合算データの改ざんをしていないか否かを判定する。これによって、店舗取引端末3における売上合算デ

6

ータの改ざんを防ぐことが可能である。

【0023】また、この第1の例において、認証子29を使用する代わりに暗号文を用いる方法がある。システム構成は、認証子29の部分が暗号文に代わるほかは、図9の第1の例と同様である。

【0024】店舗取引端末3の売上合算データ28を買物客の購買にともなって更新する際には（買物による加算）、まず、更新前の売上合算データ28を暗号化部24によって銀行鍵27を使って、暗号化し、暗号化した文と該売上合算データに対応する暗号文が一致するか否かを判定する。一致すれば売上合算データ28の改ざんはないと判定して更新処理を実行し、一致しない場合には改ざんあるいはエラーが生じたとして更新処理を行なわず、その旨をオペレータに通知する。ここでは、売上合算データ28を暗号化して対応する暗号文との一致不一致を判定したが、暗号文を使用する場合には、暗号文から元の文を逆生成（復号）することが可能なので、暗号文を銀行鍵27を使用して復号し、復号値と売上合算データ28の一致不一致を判定してもよい。この場合も一致の場合は改ざん無し、不一致の場合は改ざん有りとなすことができる。暗号化には、例えば、F E A Lアルゴリズム等を使用することが可能である。

【0025】一致して、改ざんがないと判定された場合の更新処理では、まず、店舗取引端末3のキーボード等から入力された買物金額9と売上合算データ28のデータを加算器23で加算し、再び売上合算データ28に格納する。また、加算器23の出力、すなわち、新たな売上合算データを暗号化部25に入力し、銀行鍵27で暗号化して暗号文を作成し、これを売上合算データ28に対応した暗号文として格納する（認証子29の部分を暗号文として置き換える）。

【0026】ICカード2側の処理は前記の第1の例と同一である。すなわち、店舗取引端末3に入力される買物金額9がICカード2にも送られ、この金額が金額表示部21に出力されるとともに、減算器20に入力され、減算器20では残高格納レジスタ8の値から該買物金額9を減算して、減算結果を再び残高格納レジスタ8に格納し、残高データを更新する。

【0027】図10は第2の例のシステム構成図である。売上合算データの更新処理および暗号化をICカード側で行なうものである。ICカード2には、ICカードによる合算データ暗号化部30およびICカードによるカード残高更新部31がある。ICカードによる合算データ暗号化部30は、カード・ユーザが買物をする店舗の店舗取引端末3の売上合計金額を更新するとともに、そのデータを暗号化する処理を実行し、ICカードによるカード残高更新部31は、該ICカード2の残高を更新する処理を実行する。

【0028】ICカードによる合算データ暗号化部30は、金額表示ディスプレイ21のほか、加算器32、暗

号化部33、復号部34、比較器35、銀行鍵格納部36からなる。銀行鍵格納部36には、ICカード2を発行した銀行（銀行A）の銀行鍵が格納しており、この鍵を使用して、暗号化部33では被暗号文の暗号化を行ない、復号部34では暗号文の復号を行なう。一方、ICカードによるカード残高更新部31は、上記第1の例におけるICカード2の構成と同様であり、残高格納レジスタ8および減算器20よりなる。

【0029】一方、店舗取引端末3は売上データ格納部37および加算器38、比較器39で構成する。売上データ格納部37は、取引銀行名40および売上合算データの平文41、売上合算データの暗号文42からなり、店舗取引端末3が取引している銀行ごとに分けて格納する（37-1、37-2、37-3、・・・）。そして、売上合算データ（平文41）とそれを暗号化した暗号文42を対にして売上データ格納部37に格納する。

【0030】買物客の購買によって売上合算を更新する場合には、まず、店舗取引端末3にICカード2を挿入し、店舗取引端末3のキーボード等から買物金額9を入力する。ICカード2を挿入したことで、ICカード2にICカード2を発行した銀行（ここでは銀行A）について売上データ格納部37の平文41（41-1）と暗号文42（42-1）が送られる。そして、暗号文42はICカード2内の復号部34の入力となり、ICカード2が銀行鍵格納部36に格納している銀行鍵（ここではA銀行の鍵）を使用して、復号する。これによって、暗号文42は暗号化前の平文に戻るはずである。復号化済みの文は比較器35の入力となる。比較器35のもう一つの入力は、店舗取引端末3から送られた平文41である。比較器35は復号化済みの文と店舗取引端末3からの平文41を比較し、一致していれば店舗取引端末3側での売上データの改ざんはないとみなし、売上合算データの更新処理を行なう。一方、一致していない場合には、復号化した文と元の平文が異なるということで、何らかの改ざんあるいはエラーが発生したものとオペレータにその旨を通知し、処理を終了する。

【0031】比較器35の結果が一致で、改ざんされていない場合には、店舗取引端末3から送られてきた売上データ格納部37内の平文41の値と、キーボードで入力した買物金額9を加算器32に入力する。加算器32はこれらの二つの値を加算して売上合算金額を求める。この結果は、店舗取引端末3に送られるとともに、ICカード2内にある暗号化部33に送られる。暗号化部33は、銀行鍵格納部36に格納されている銀行鍵によって売上合算金額を暗号化し、その結果を暗号文更新データ43として店舗取引端末3に送る。店舗取引端末3では、受け取った暗号文更新データ43を売上データ格納部37の暗号文42に格納する。

【0032】一方、ICカード2内の加算器32の出力（売上合算金額）は店舗取引端末3にも送られ、店舗取

引端末3内の比較器39の一方の入力となる。また、店舗取引端末3内にも加算器38が存在し、売上データ格納部37の売上データの平文41と買物金額9を加算し、独自に売上合算金額を算出し、これを比較器39のもう一方の入力とする。ICカード2から送られてきた売上合算金額と、店舗取引端末3で独自に計算した売上合算金額とが一致すれば、正しく計算されているものとして、該売上合算金額を金額更新データ44として売上データ格納部37の平文41に格納する。一方、比較器39で不一致になれば、ICカード2から送られてきた売上合算金額と、店舗取引端末3で独自に計算した売上合算金額とが異なることになり、ICカード2側あるいは店舗取引端末3側のいずれか、あるいは両方でエラーが発生していることになる。このような場合には処理を停止し、その旨を出力する。

【0033】ICカード2では、店舗側の売上合算データ更新処理に加えて、自身の残高更新処理も行なう。ICカードによるカード残高更新部31は、残高格納レジスタ8に格納してある残高データを減算器20に入力する。そして、減算器20のもう一方の入力を買物金額9とし、残高データから買物金額9を減算して、再び残高格納レジスタ8に格納する。これにより、残高データの更新が完了する。

【0034】この第2の例は、店舗側の売上合算計算処理および売上合算の暗号化をICカード側で行ない、店舗側では処理できないようにしている。前記の第1の例では、銀行鍵を店舗側で読取すれば売上合算計算およびその暗号化が可能で、不正改ざんの可能性が残されていたが、この第2の例のように、ICカード側で処理させることにより、このような不正行為は防止できるようになる。また、銀行ごとに銀行鍵を変えることにより、その銀行が発行したICカードでないと暗号化処理が行なえず、安全性が増すとともに、銀行鍵の更新を銀行ごとに行なえるという利点がある。

【0035】なお、この第2の例は、暗号化処理により、売上合算データの平文41とともに対応する暗号文42を売上データ格納部37に格納したが、売上合算データの平文41の一部を使用して暗号化することにより、対応する認証子を暗号文42のところに格納する方法を採ってもよい。

【0036】ところで、図11は前述の第1あるいは第2の例のシステム構成で求め、店舗取引端末に格納された売上合算データで発生し得る不正の説明図である。店舗取引端末3に蓄積されている売上データ22は、一定期間内の売上合算データ28と、該売上合算データ28に暗号化処理を施して得られた認証子29からなる。今、ある月の売上合算データ28が100万円であったとする。そして、その月には、この売上合算金額を銀行センタ4に請求する（第n回請求データ48）。即ち、第n回請求データ48は売上合算データ28（100万

円)と対応する認証子29である。銀行センタ4はこのデータを受け取り、まず、暗号化部45が売上合算データ28を銀行鍵46で暗号化する。この暗号化で得た認証子を比較器47に入力し、送られてきた認証子29と比較する。これが一致していれば不正はないと判定し、銀行センタ4は請求額を店舗口座に入金する。

【0037】ここで、次の月の売上合算金額が例えば10万円と少なく、売り上げの水増しを図るために、店舗側取引端末3でこの月の売上データ22として前月の売上データ22をそのまま複写する不正改ざんをするものとする。すなわち、前月の売上合算データ28(100万円)と対応する認証子29を今月の売上データ22として複写する。

【0038】このような場合、第n+1回請求データ49として複写した前月の売上データ22がそのまま銀行センタ4に送られる。すなわち、売上合算データ28(100万円)とそれに対応する認証子29が送られる。銀行センタ4では、送られてきた第n+1回請求データ49の売上合算データ28を銀行鍵46で暗号化し、認証子29と比較する。しかし、送られてきた売上合算データ(100万円)28と認証子29は対応がとれているので、前月のデータを複写したことは検出できず、このような不正を防ぐことができない。このような、複写による不正は銀行センタ4への請求時でも、月の途中でも、いつでも可能である。

【0039】これは、売上合算データと認証子が1対1に対応していることによる。このような不正を防ぐために、売上データ22に請求のシリアル番号を付加する方法が考えられる。

【0040】図12は第三の例、すなわち、売上データにシリアル番号を付加したシステムの説明図である。店舗取引端末3は銀行センタ4への売上請求ごとにインクリメントされるカウンタを有しており、銀行センタ4には各店舗取引端末に対応したシリアル番号がチェック用カウンタ51として格納されている。そして、請求データとしては売上合算データ28および認証子29を送る。この認証子29は、売上合算データ28にシリアル番号50を付加したデータをICカード2が暗号化して得たものである。

【0041】例えば、2回目の請求データは売上合算データ28の値が「100万円」であり、また、認証子29はシリアル番号「2」と売上合算データ「100万円」を合わせたデータを暗号化して得た認証子である。銀行側では、2回目の請求であることをチェック用カウンタ51で検出し、これと送られてきた売上合算データ「100万円」を合わせて暗号化し認証子を得て、店舗取引端末3から送られてきた認証子と比較する。一致していれば不正はないと判断して請求額を店舗口座に入金する。不一致ならば不正またはエラーがあると判断する。

【0042】ここで、3回目の請求時に売上が少なく、店舗側取引端末3で前回の請求データを複写する不正を行なうものとする。すなわち、売上合算データ「100万円」と認証子を複写する。銀行センタ4に請求すると、チェック用カウンタ51により、銀行側は3回目の請求であることを検出し、シリアル番号「3」と売上合算データ「100万円」を合わせて暗号化し認証子を求め、店舗取引端末3から送られてきた認証子と比較する。この場合、送られてきた認証子はシリアル番号「2」として暗号化したものであり、銀行センタ3で求めた認証子とは一致しない。これにより不正が検出できる。

【0043】この第三の例では、銀行への請求回数を示すシリアル番号を売上合算データに加えて暗号化を行なったが、シリアル番号の代わりに合算開始時の日時を用いても実現できる。店舗取引端末3では、合算開始時の日時を売上合算データ28に付加し、認証子を生成する。銀行センタ4では、前回の請求時に送られてきた売上合算データに付加されていた日時を店舗取引端末ごとに管理しており、今回請求された売上データに付加されている日時と比較する。日時が同じであったり、前回の請求時の日時よりも古いならば不正があると判断される。日時が新しいならば、日時と売上合算データを合わせて暗号化し、認証子を生成し、店舗取引端末から送られてきた認証子と比較し、一致していれば決済処理を行なう。一致しない場合には、何らかの不正あるいはエラーがその他にも存在すると判断され、決済処理は行なわない。

【0044】図13は第三の例までのシステムでも起こり得る不正の説明図である。店舗側に複数台の店舗取引端末があるとする(3-1, 3-2)。店舗取引端末A3-1の売上合算データ28-1が100万円であり、店舗取引端末B3-2の売上がったデータ28-2が100万円であるとする。それぞれの認証子(29-1, 29-2)は、それぞれの売上合算データ(28-1, 28-2)を暗号化して得たものである。

【0045】ここで、店舗取引端末B3-2の売上が少ないので、店舗取引端末A3-1の売上データ22-1を複写して水増しする不正を行なうものとする。これによって、店舗取引端末B3-2の売上データ22-2には、店舗取引端末A3-1の売上データ22-1がそのまま複写され、店舗取引端末B3-2の売上も100万円ということになる。この請求データ61を銀行センタ4に送ると、銀行センタ4の暗号化部45が店舗取引端末Bの請求データ61中の売上合算データ28-2(100万円)を銀行鍵46で暗号化し、その結果を比較器47で送られてきた認証子29-2と比較する。銀行センタ4は、請求データ61からは店舗取引端末の違いを検出することができないので、比較器47では一致すると判定され、決済処理が実行される。以上のように、他

11

の店舗取引端末の売上合算を複写することにより売り上げを水増しする不正が起こり得るのである。

【0046】図14は第4の例、すなわち、店舗取引端末のIDを付加するシステムの説明図である。店舗取引端末にはユニークなIDが与えられており、売上データ22に店舗取引端末ID70として含め、銀行センタ4に請求する。銀行センタ4では各端末のIDを管理している（端末番号71）。

【0047】各店舗取引端末では、売上合算データ28に端末ID70を付加したデータに対しての認証子29をICカードにより計算し、格納する。銀行センタ4に売上請求を行なう場合には、売上合算データ28と認証子29を送る。銀行センタ4では、同一の店舗取引端末IDをもつ売上請求があるか否かを判定し、同じIDの付いた請求があれば不正があると判断する。同じIDの付いた請求がないならば、送られてきた売上合算データ28を暗号化部で暗号化し、得た認証子を店舗取引端末から送られてきた認証子と比較する。一致していれば不正はないものとして決済処理を行なう。一致しない場合には、何らかの不正あるいはエラーがあるものとして決済処理を行なわないようにする。

【0048】これによって、ATM等の入金端末、店舗取引端末での不正が困難になり、安全性を向上することが可能である。さらに、これまで安全性の面で換金性のないプリペイドカード（目的が限られたプリペイドカード）しか発行できなかったが、換金性をもつICカードが発行可能となり、キャッシュレス・システムの使用範囲が広がる。

【0049】このようにして、カードを発行する銀行センタ及びICカードを信頼点として電子財布システムを構築してきたが、万一のICカードの不正な複製が可能となった場合、被害が拡大するおそれがあり、このためシステムの安全性向上が必要とされている。

【0050】ところで、ICカードに書き込まれた秘密の鍵が、カードを発行した銀行管理の鍵（銀行鍵）と共通で、その銀行と取引する顧客のカードの鍵が全て共通であったとすると、ICカードの格納された鍵が漏洩した場合、その銀行の顧客全体に被害が拡大するおそれがある。

【0051】本発明は、このような課題に鑑み創案されたもので、銀行鍵を個人毎にユニークにし、更にこれを時間可変な鍵とすることによって、高い安全性を確保できるようにした、電子財布システムの鍵管理方式を提供することを目的とする。

【0052】

【課題を解決するための手段】図1は本発明の原理説明図で、この図1に示す電子財布システムの鍵管理方式は、次のようなステップをとる。

(1) 現金自動支払い装置4AとICカード2との間でのステップST1。

12

すなわち、このステップST1では、まず、銀行センタ4で、マスタ鍵を用いて、この銀行センタ4が生成する第1のパラメータを暗号化し、この銀行センタ4より現金自動支払い装置4Aを経由してユーザのICカード2へ配送するが、次に、ユーザは現金自動支払い装置4Aより配送された暗号化パラメータをICカード2に取り込み、ICカード2内のマスタ鍵Lを用いて復号部2-1で復号し、銀行発行の第1のパラメータを得、更にこのパラメータとユーザが管理するパスワードPWとを、ICカード2内の加算部2-2で加算し、この結果を第1のレジスタ2-3に書き込む。

【0053】(2) ICカード2と店舗取引端末3との間でのステップST2。

すなわち、このステップST2では、ユーザが商店で買物を行ない、店舗取引端末3で買物金額を支払う際に、ICカード2を店舗取引端末3のカードリーダーへ挿入して、店舗取引端末3側で予め銀行センタマスタ鍵で暗号化した第2のパラメータをICカード2に対して送ると、ICカード2は受信した第2の暗号化パラメータを内蔵のマスタ鍵Lを用いて、復号部2-1'で復号し、得られた第2のパラメータを第1のレジスタ2-3の値に対して加算部2-2'で加算し、その結果を第2のレジスタ2-4に格納するが、更にICカード2内のメモリ2-5に記憶された暗号化セッション鍵を用いて、第2レジスタ2-4の値を用いて復号部2-1''で復号し、目的の認証用の鍵KBajを得る。

【0054】さらに詳しくは、ICカード2内のメモリ2-5に、暗号化セッション鍵を複数種類記憶しておき、ICカード2が店舗取引端末3側から第2の暗号化パラメータを受け取る際に、メモリ回路2-5のアドレス情報を有する通番情報を受け取り、この通番情報に対応するメモリ2-5のアドレスをアクセスして、対応するアドレスに記憶された暗号化セッション鍵を出力して、第2レジスタ2-4の値でこの出力を復号し、目的の認証用の鍵KBajを得る。

【0055】(3) ICカード2への暗号化鍵補給配送ステップST3。

このステップST3では、ICカード2のメモリ2-5へ一連の暗号化セッション鍵を書き込む場合、銀行センタ4よりマスタ鍵で暗号化セッション鍵を暗号化し、このデータを現金自動支払い装置4Aを通じて、ICカード2に与え、ICカード2は受信したデータをマスタ鍵Lを用いて復号部2-1'''で復号し、得られた一連の暗号化セッション鍵データを順次メモリ2-5に格納する。

【0056】(4) その他

銀行センタ2が暗号化セッション鍵を発行する場合、一定の時間単位に対応する複数個の暗号化セッション鍵を現金自動支払い装置4A経由でICカード2に配送したり、銀行センタ2が店舗取引端末3に対して第2の暗号

13

化パラメータを送る場合、銀行センタ2よりマスタ鍵で暗号化した第2のパラメータを一定の時間単位に対応させて複数個のデータを店舗取引端末3へ送ったりしてもよい。

【0057】

【作用】上述の本発明の電子財布システムの鍵管理方式では、図1に示すように、まず、銀行センタ4で、マスタ鍵を用いて、この銀行センタ4が生成する第1のパラメータを暗号化し、この銀行センタ4より現金自動支払い装置4Aを経由してユーザのICカード2へ配送して、ユーザが現金自動支払い装置4Aより配送された暗号化パラメータをICカード2に取り込み、ICカード2内のマスタ鍵を用いて復号部2-1で復号し、銀行発行の第1のパラメータを得、更にこのパラメータとユーザが管理するパスワードPWとを、ICカード2内の加算部2-2で加算し、この結果を第1のレジスタ2-3に書き込む（ステップST1参照）。

【0058】その後、ユーザが商店で買物を行ない、店舗取引端末3で買物金額を支払う際に、ICカード2を店舗取引端末3のカードリーダーへ挿入して、店舗取引端末3側で予め銀行センタマスタ鍵で暗号化した第2のパラメータをICカード2に対して送るが、このICカード2は受信した第2の暗号化パラメータを内蔵のマスタ鍵を用いて、復号部2-1'で復号し、得られた第2のパラメータを第1のレジスタ2-3の値に対して加算部2-2'で加算し、その結果を第2のレジスタ2-4に格納して、更にICカード2内のメモリ2-5に記憶された暗号化セッション鍵を用いて、第2レジスタ2-4の値を用いて復号部2-1''で復号し、目的の認証用の鍵K B a jを得る（ステップST2参照）。

【0059】さらに詳しくは、ICカード2内のメモリ2-5に、暗号化セッション鍵を複数種類記憶しておき、ICカード2が店舗取引端末3側から第2の暗号化パラメータを受け取る際に、メモリ回路2-5のアドレス情報を有する通番情報を受け取り、この通番情報に対応するメモリ2-5のアドレスをアクセスして、対応するアドレスに記憶された暗号化セッション鍵を出力して、第2レジスタ2-4の値でこの出力を復号し、目的の認証用の鍵K B a jを得るのである（ステップST2参照）。

【0060】ところで、ICカード2のメモリ2-5へ一連の暗号化セッション鍵を書き込む場合は、銀行センタ4よりマスタ鍵で暗号化セッション鍵を暗号化し、このデータを現金自動支払い装置4Aを通じて、ICカード2に与え、ICカード2は受信したデータをマスタ鍵を用いて復号部2-1'''で復号し、得られた一連の暗号化セッション鍵データを順次メモリ2-5に格納する（ステップST3参照）。

【0061】なお、銀行センタ2が暗号化セッション鍵を発行する場合、一定の時間単位に対応する複数個の暗

14

号化セッション鍵を現金自動支払い装置4A経由でICカード2に配送したり、銀行センタ2が店舗取引端末3に対して第2の暗号化パラメータを送る場合、銀行センタ2よりマスタ鍵で暗号化した第2のパラメータを一定の時間単位に対応させて複数個のデータを店舗取引端末3へ送ったりしてもよい。

【0062】

【実施例】以下、図面を参照して本発明の実施例を説明する。図6は本発明の一実施例を示す全体ブロック図で、この図6に示す電子財布システムは、銀行センタ4、現金自動支払い装置（ATM）4A、ICカード2及び店舗取引端末（POS端末）3から構成されている。

【0063】ところで、本電子財布システムの鍵管理方式は、現金自動支払い装置4AとICカード2と間での鍵生成パラメータ配送処理、ICカード2と店舗取引端末3と間での鍵生成パラメータ配送処理、ICカード2への暗号化鍵補給配送処理等に分けて説明できるが、以下各処理について詳述する。

【0064】図2は顧客がATM4Aを経由して可変銀行鍵KBを復号する為の鍵KIDiを生成するのに必要なパラメータKcentを配送してもらう処理を示している。この図2において、最初に顧客IDiは本人所有のICカード（電子財布）2をATM4Aにさしこむ（図2の①）。このとき、ICカード2より顧客のID番号が自動的に銀行センタ4へ送られ、銀行センタ4は送られてきたID番号を鍵テーブルのアドレスとして顧客の通信鍵Liを索引する。銀行センタ4はこの鍵Liを使って秘密パラメータKcentを暗号化し、顧客IDiのICカード2へ配送する（図2の②）。この手段により、銀行センタ4、ATM4A間の通路の不在改ざんを防止することができる。

【0065】一方、ICカード2側では、カード内蔵の鍵Liで暗号化パラメータを復号部2-1で復号し、Kcentを得る（図2の③）。次に、顧客のパスワードPWiとの先のKcentとを加算部2-2で加算し、第2のパラメータSi（=Kcent+PWi）を作り、レジスタ2-3に格納する（図2の④）。

【0066】図3は、顧客が店で買物を行ない、買物代金をICカード2で支払うときの、ICカード2と店のPOS端末3と間の処理を示している。この図3において、顧客がICカード2をPOS端末3のカードリーダーに挿入すると、ICカード2よりID番号がPOS端末3へ自動的に送出され、POS側のセキュリティブロックボックス（BB）3-11より鍵LiでKbbを暗号化したデータELi（Kbb）が配送されてくる（図3の①）。ここで、ELi（Kbb）は銀行センタ4よりPOS端末3へ事前に配送しておく。

【0067】一方、ICカード2側ではカード内蔵の鍵Liで暗号化パラメータを復号部2-1'で復号し、K

15

bbを得る(図3の②)。このKbbとレジスタ2-3の格納データS1とを加算部2-2'で加算し、KIDi(=Kbb+Kcent+PWi)を得る(図3の③)。

【0068】次に、POS側セキュリティブラックボックス(BB)3-11'よりシリアル番号(通番)jがICカード2に対して送られ(図3の④)、ICカード2側では鍵KIDiで暗号化したj番目の銀行鍵KBajをメモリ(レジスタ)2-5から索引して(図3の⑤)、更にこのデータをKIDiで復号部2-1''で復号して、銀行鍵KBajを得る(図3の⑥)。

【0069】そして、このようにして鍵KBajが得られると、前記の図9~図14で説明したシステムを用いて、前述したその後の所望の処理を行なう。なお、カード内蔵の鍵LiはROMに格納され、S1格納用のレジスタ2-3、メモリ2-5としてはバッテリバックアップレジスタが使用され、KIDi格納用のレジスタ2-4、KBaj用のレジスタ2-6としてはノンバックアップレジスタが使用される。そして、レジスタ2-4、2-6の内容は買物終了段階でPOS側の指示により消去される。

【0070】図4は銀行センタ4からICカード2への鍵の補給処理を示している。顧客が金額データを補給する際に銀行センタ4より鍵の補給を受ける。この図4において、図2と同様に、ATM4Aに挿入されたICカード2は銀行センタ4より、鍵Liで暗号化した暗号化銀行鍵ELi(EKIDi(KBai))~ELi(EKIDi(KBan))を配送してもらう(図4の①)。ICカード2側では、鍵Liを用いて復号部2-1''でこれらのデータを復号して、そのデータをメモリ2-5に格納する(図4の②)。

【0071】そして、銀行センタ2が上記のように暗号化セッション鍵を発行する場合は、一定の時間単位(時間単位、日単位、週単位、月単位、年単位)に対応する複数個の暗号化セッション鍵を現金自動支払い装置4A経由でICカード2に配送する。今、顧客に発行する銀行鍵の変更周期例を示すと、図5のようになる。この例では、配送される鍵は発行日から常に1年分だけもらうようになっている。

【0072】なお、銀行センタ2が店舗取引端末3に対して第2の暗号化パラメータを送る場合、銀行センタ2よりマスタ鍵で暗号化した第2のパラメータを一定の時間単位(時間単位、日単位、週単位、月単位、年単位)に対応させて複数個のデータを店舗取引端末3へ送ってもよい。

【0073】このように、ICカード内蔵の銀行鍵(マスタ鍵)を個人ID又はカード発行時の時刻をIDとするもの等に対応する鍵を生成するメカニズムを電子財布システムに導入することにより、銀行鍵を個別化、可変化することができ、これにより万一の場合の各種カード

16

偽造行為に対して、カードシステムの安全性向上に寄与するところが大きい。

【0074】

【発明の効果】以上詳述したように、本発明の電子財布システムの鍵管理方式によれば、銀行鍵を個別化、可変化することができ、これにより万一の場合の各種カード偽造行為に対してカードシステムの安全性向上において寄与するという利点がある。

【図面の簡単な説明】

【図1】本発明の原理説明図である。

【図2】本発明の一実施例における現金自動支払い装置とICカードとの間での鍵生成パラメータ配送処理要領を説明する図である。

【図3】本発明の一実施例におけるICカードと店舗取引端末との間での鍵生成パラメータ配送処理要領を説明する図である。

【図4】本発明の一実施例におけるICカードへの暗号化鍵補給配送処理要領を説明する図である。

【図5】顧客に発行する銀行鍵の変更周期例を説明する図である。

【図6】本発明の電子財布システムの概略を示すブロック図である。

【図7】従来方式によるICカードを用いたプリペイドカード・システムの構成図である。

【図8】従来の店舗側の取引端末の売上合算データの更新とICカード残高の更新の説明図である。

【図9】店舗側の取引端末での売上合算データの更新を説明するシステム構成図である。

【図10】買物客のICカードによる売上合算データの更新を説明するシステム構成図である。

【図11】前回請求データの複写による売上の水増しの説明図である。

【図12】店舗売上データへのシリアル番号の付加説明図である。

【図13】他の店舗取引端末の請求データの複写による売上の水増しの説明図である。

【図14】店舗売上データへの取引端末IDの付加説明図である。

【符号の説明】

2 ICカード

2-1, 2-1', 2-1'', 2-1''' 復号部

2-2, 2-2' 加算部

2-3 第1のレジスタ

2-4 第2のレジスタ

2-5 メモリ

2-6 レジスタ

3 店舗取引端末

3-11, 3-11' セキュリティブラックボックス

4 銀行センタ

4A 現金自動支払い装置(ATM)

17

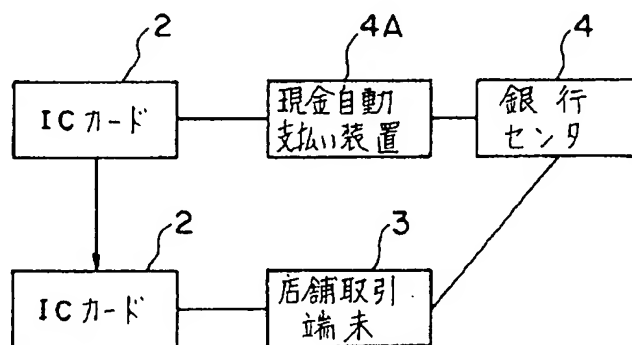
8 残高格納レジスタ
 20 減算器
 20 金額表示部
 21 金額表示部
 22 売上データ
 23 加算器
 24、25 暗号化部
 26 比較器
 27 銀行鍵
 30 合算データ暗号化部
 31 ガード残高更新部
 32 加算器
 33 暗号化部
 34 復号部
 35 比較器
 36 銀行鍵格納部
 37 売上データ格納部

18

38 加算器
 39 比較器
 45 暗号化部
 46 銀行鍵
 47 比較器
 81 ICカード
 82 店舗取引端末
 83 銀行センタ
 84 個人口座
 10 85 個人カード残高ログファイル
 86 未決済資金ファイル
 87 店舗口座
 88 残高格納レジスタ
 96 加算器
 97 減算器
 98 金額表示ディスプレイ

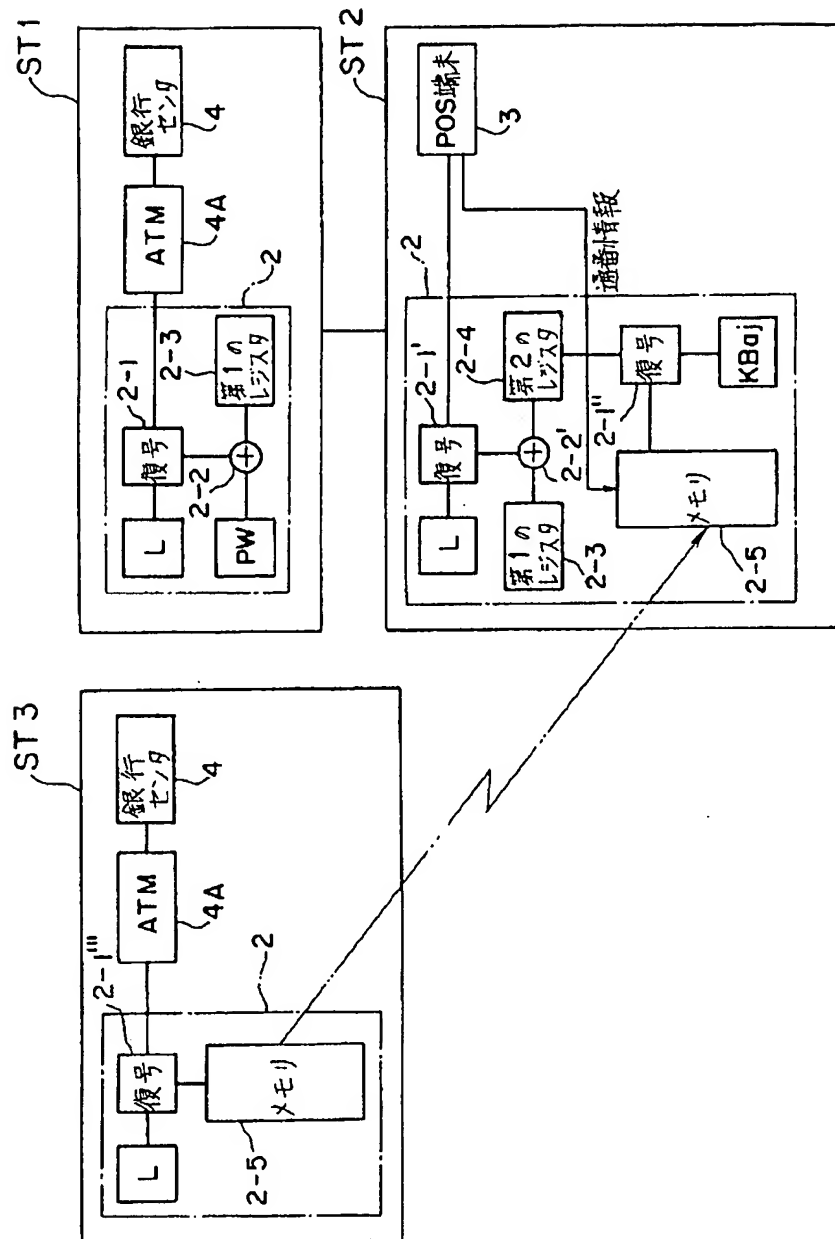
【図6】

本発明の電子財布システムの概略を示すブロック図



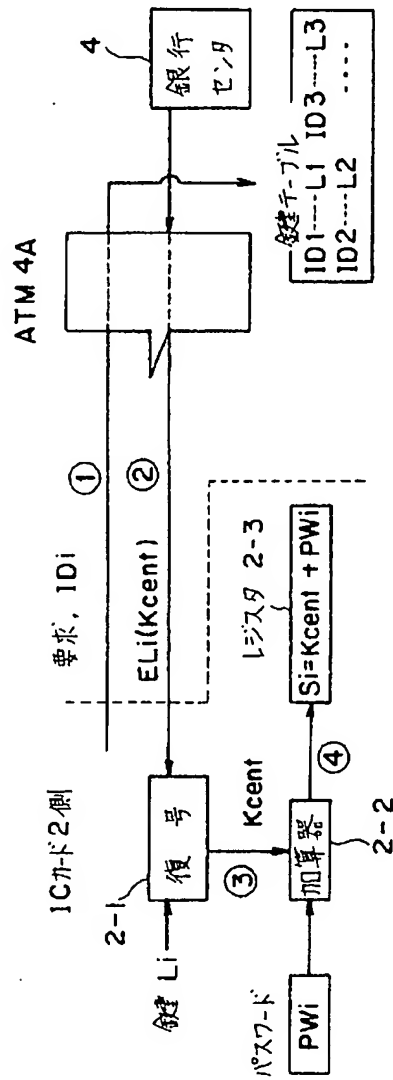
【図1】

本発明の原理説明図



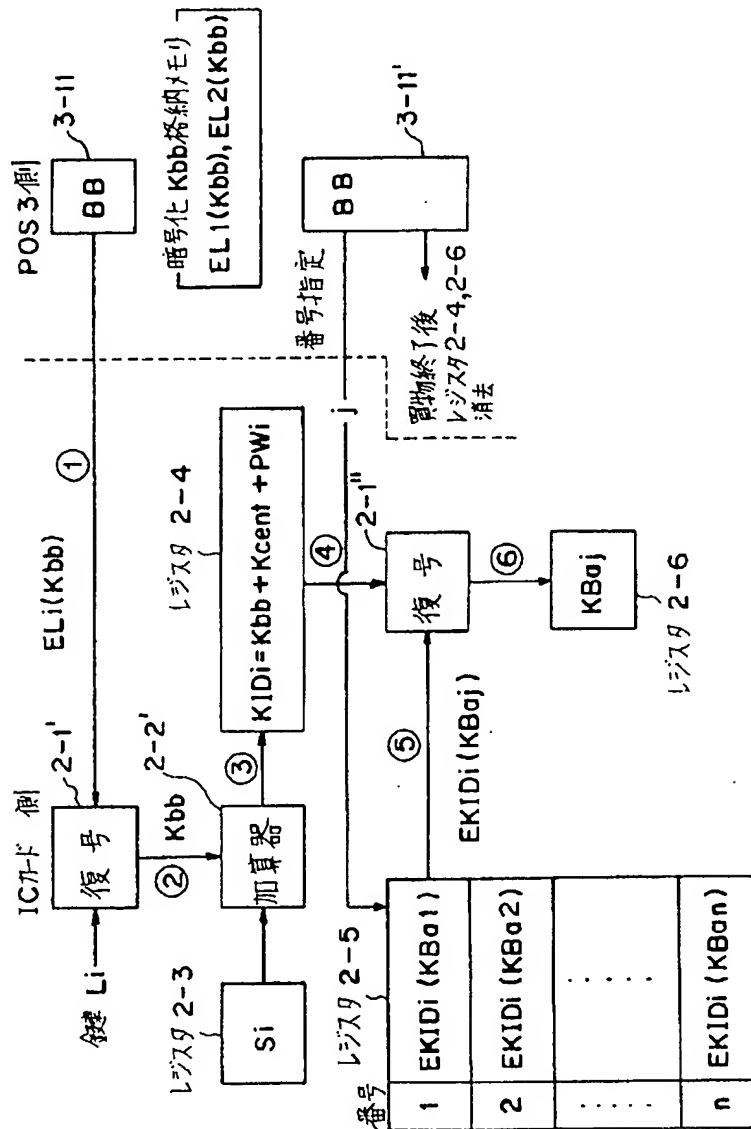
【図2】

本発明の一実施例における現金自動支払い装置とICカードとの間の鍵生成パラメータ配送処理要領を説明する図



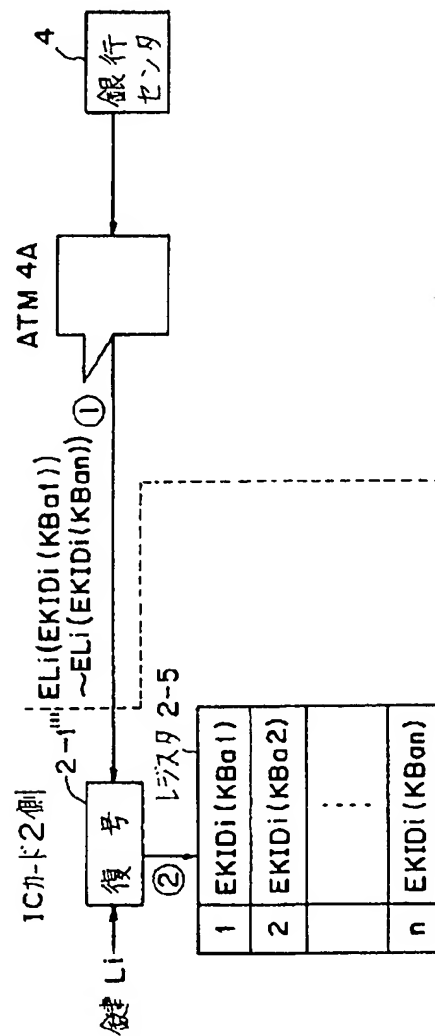
【図3】

本発明の一実施例におけるICカードと店舗取引端末との間での鍵生成パラメータ配送処理要領を説明する図



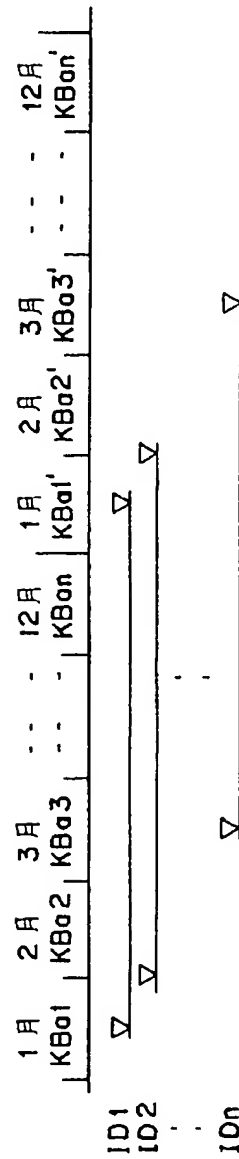
【図4】

本発明の一実施例におけるICカードへの暗号化
鍵補給配送処理要領を説明する図



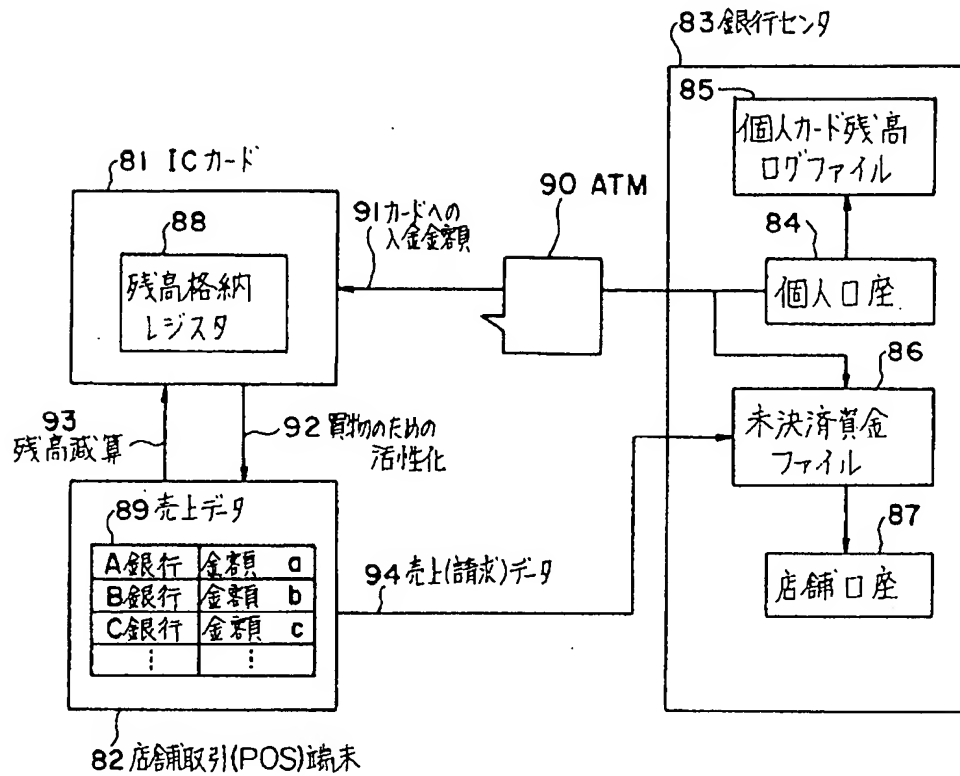
【図5】

顧客に発行する銀行鍵の変更周期例を説明する図



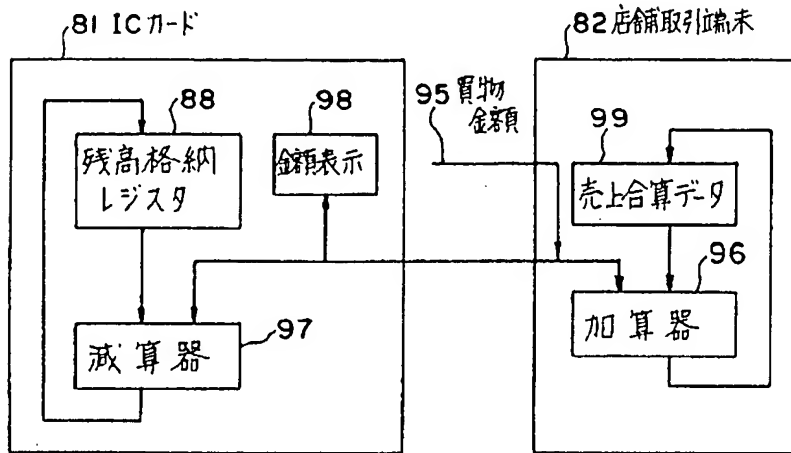
【図7】

従来方式によるICカードを用いたプリペイドカードシステムの構成図



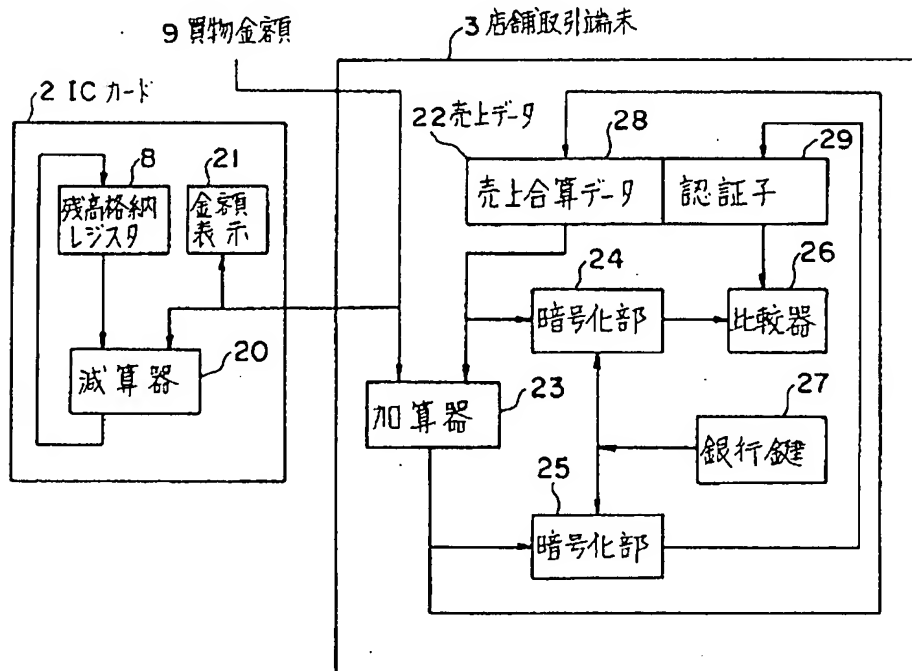
【図8】

従来の店舗側の取引端末の売上合算データの更新と
ICカード残高の更新の説明図



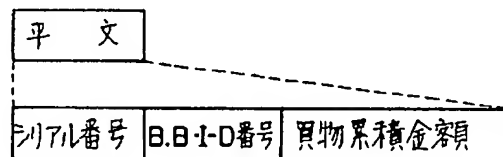
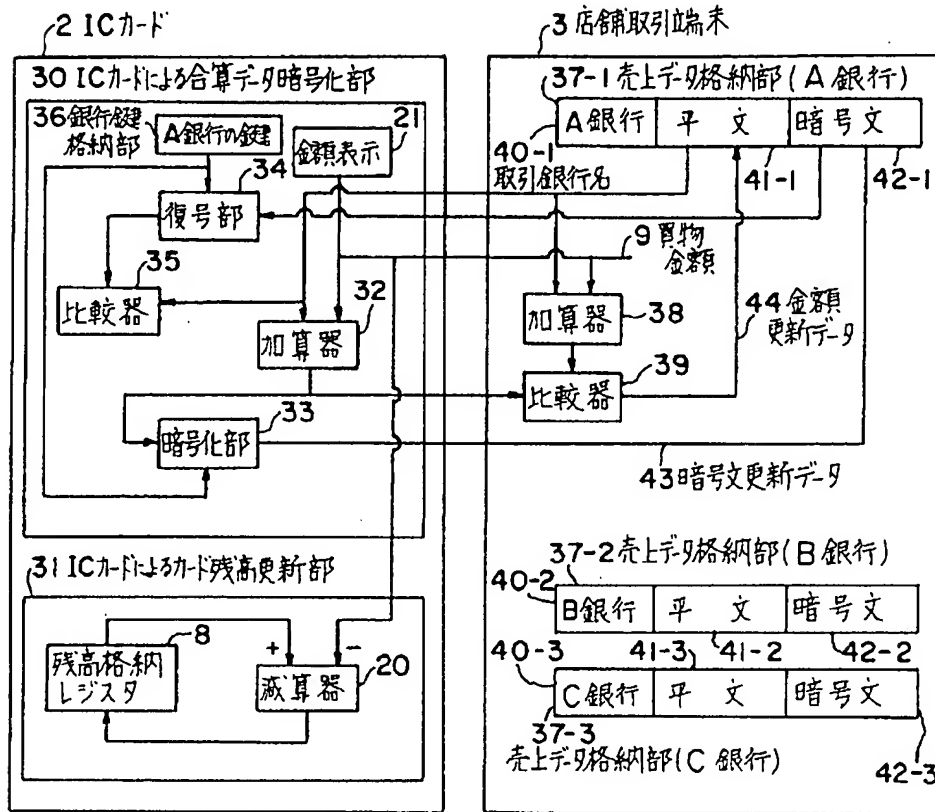
【図9】

店舗側の取引端末での売上合算データ更新例を説明する
システム構成図



【図10】

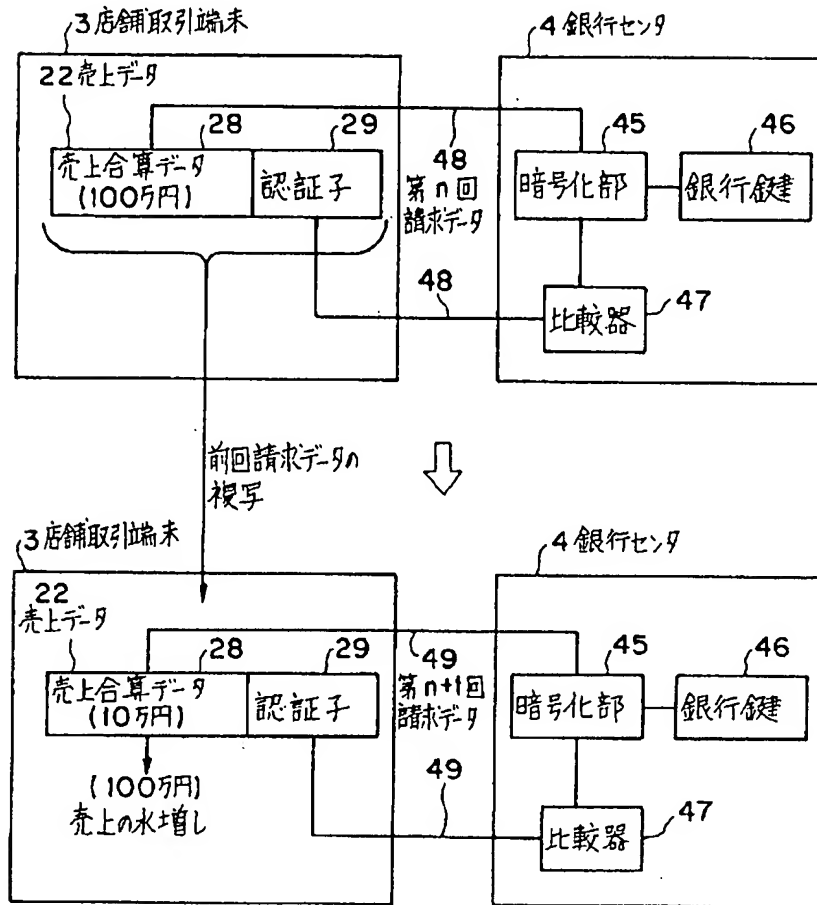
買物客のICカードによる売上合算データの更新を説明する
システム構成図



シリアル番号：前回締め上げの以前のデータの利用防止のための
シリアル番号. 締め上げの度にインクリメントされる。
B.B-I-D番号：他のブラックボックスの買物累積金額の利用防止
のためのID。

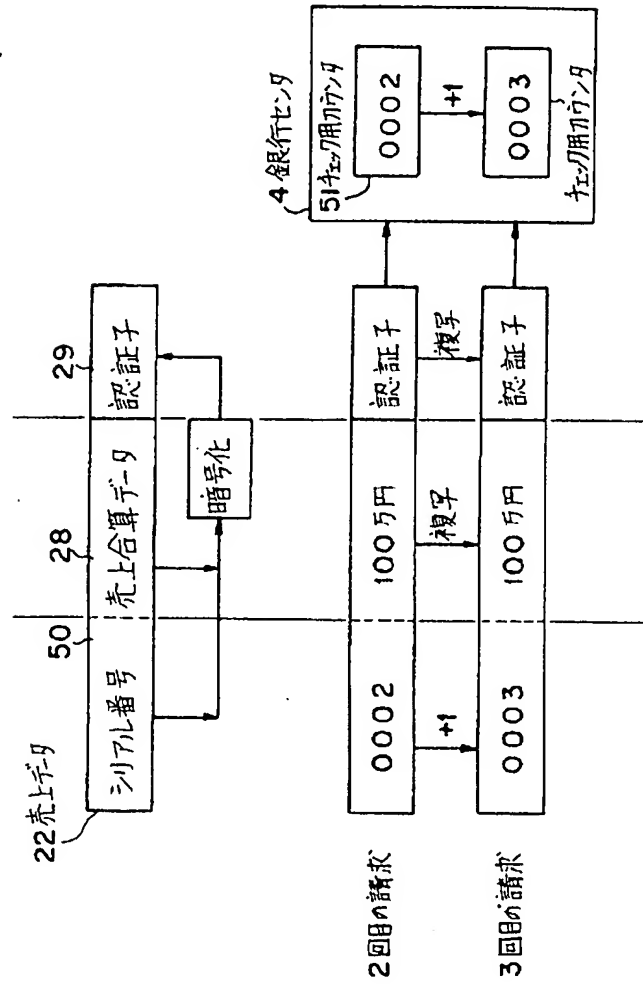
【図11】

前回請求データの複写による売上の水増しの説明図



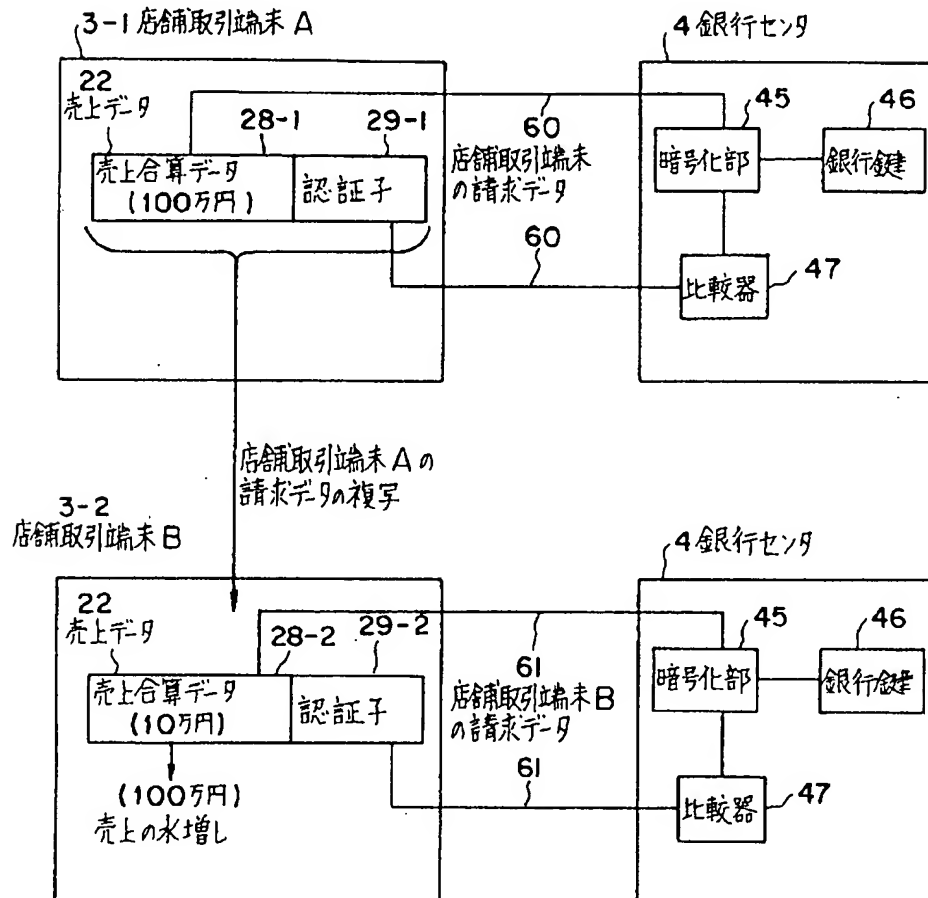
【図12】

店舗売上データのシリアル番号の付加説明図



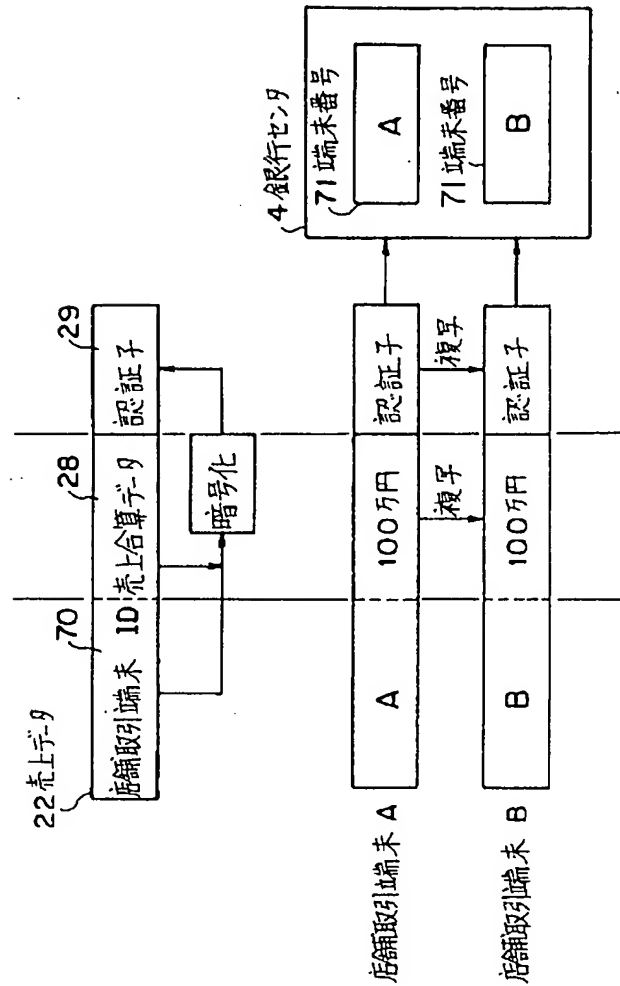
【図13】

他の店舗取引端末の請求データの複写による売上の水増しの説明図



【図 1 4】

店舗売上データへの取引端末 ID の付加説明図



フロントページの続き

(51) Int. Cl.⁵

G 0 7 D 9/00

G 0 7 F 7/12

G 0 7 G 1/14

H 0 4 L 9/28

識別記号

4 6 1 B 8513-3E

庁内整理番号

8921-3E

F I

技術表示箇所